Exam : 200-201

Title : Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

https://www.passcert.com/200-201.html

1.An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network.

What is the impact of this traffic?

A. ransomware communicating after infection

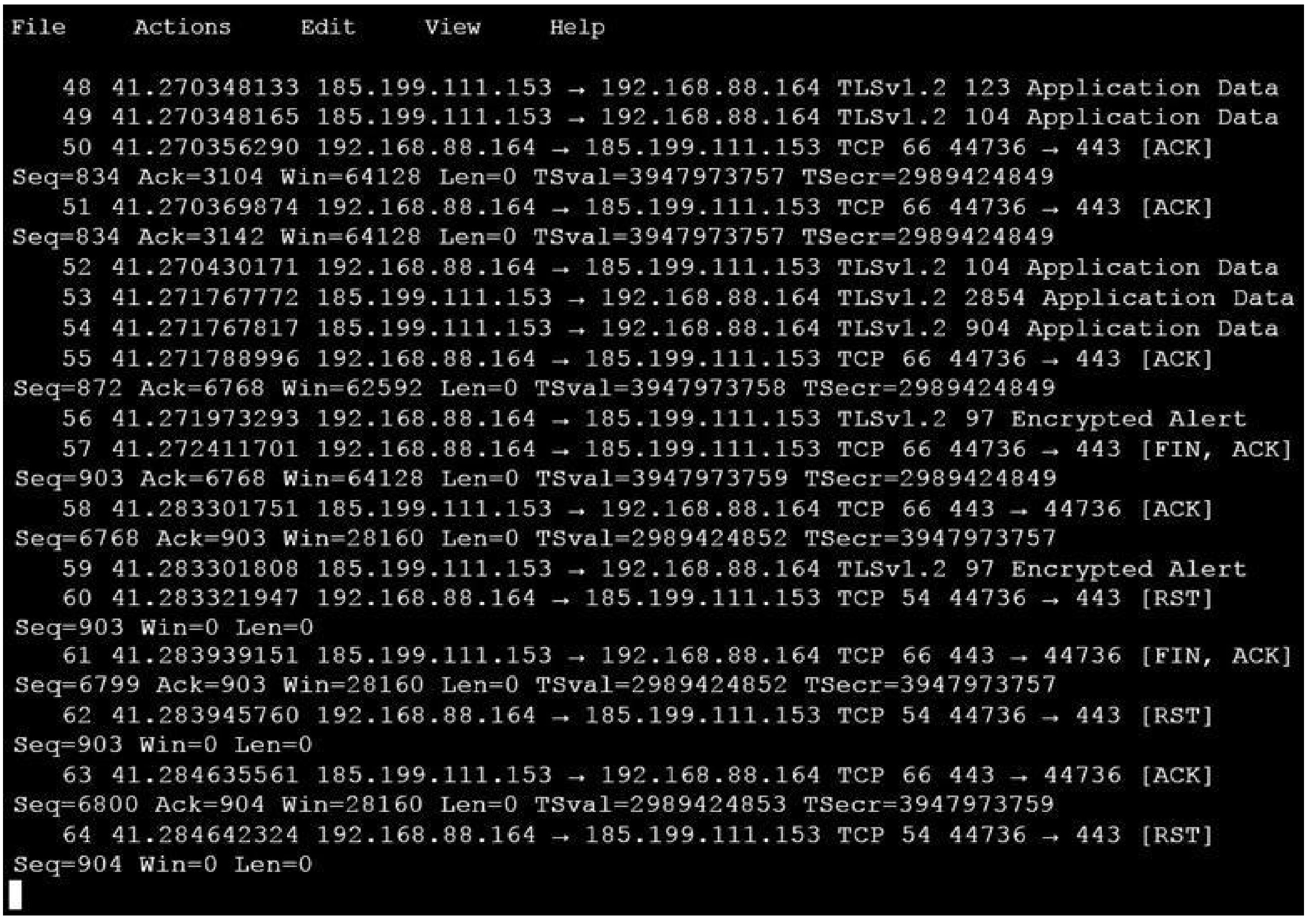
B. users downloading copyrighted content

C. data exfiltration

D. user circumvention of the firewall

Answer: D

2.An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.



```
   48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
   49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
   50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
   53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
   54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
   55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
   56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
   57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
   58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
   60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
   64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

Which obfuscation technique is the attacker using?

A. Base64 encoding

B. TLS encryption

C. SHA-256 hashing

D. ROT13 encryption

Answer: B

Explanation:

ROT13 is considered weak encryption and is not used with TLS (HTTPS:443). Source: https://en.wikipedia.org/wiki/ROT13

3.Which technology on a host is used to isolate a running application from other applications?

A. sandbox

B. application allow list

C. application block list

D. host-based firewall

Answer: A

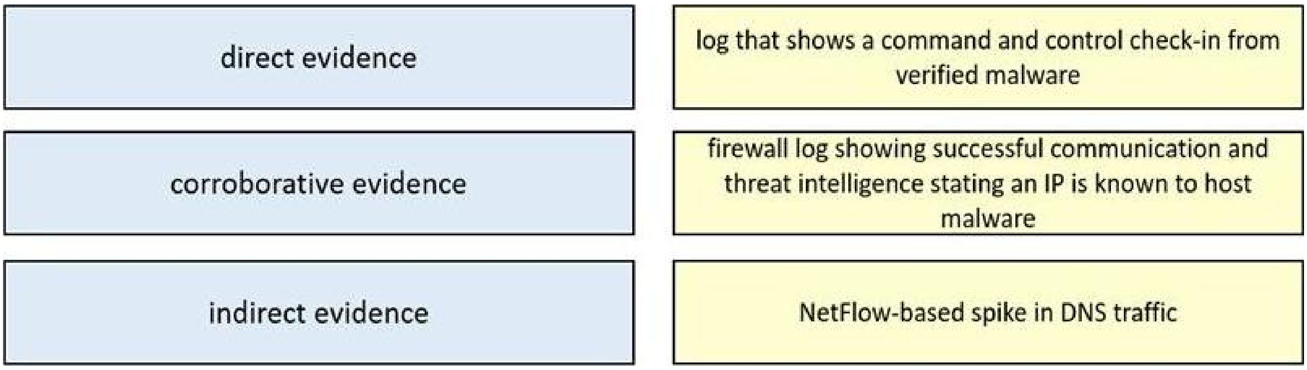
Explanation:

Reference:

https://searchsecurity.techtarget.com/definition/sandbox#:~:text=Sandboxes%20can%20be%20used%20to,be%20run%20inside%20a%20sandbox

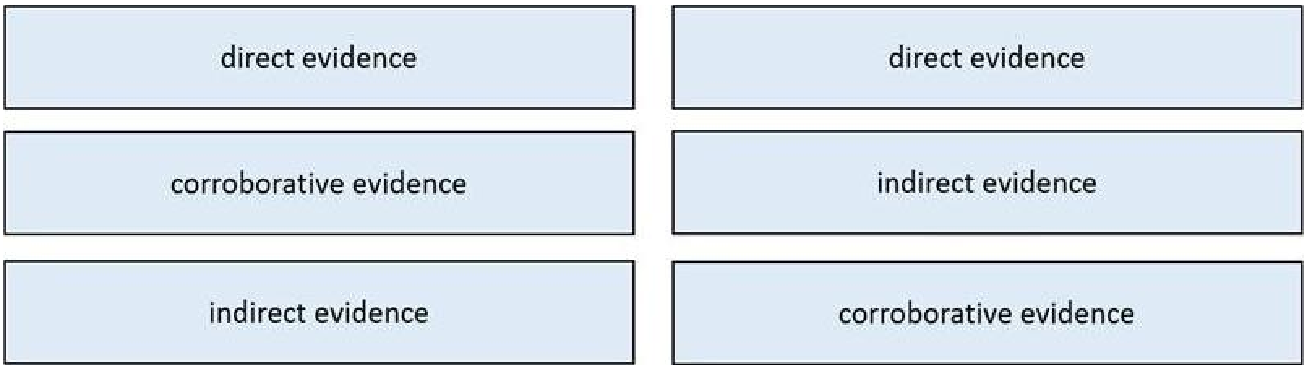
4.DRAG DROP

Drag and drop the type of evidence from the left onto the description of that evidence on the right.



direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

Answer:



direct evidence	direct evidence
corroborative evidence	indirect evidence
indirect evidence	corroborative evidence

Explanation:

Graphical user interface, application

Description automatically generated

5.How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.

B. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.

C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.

D. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Answer: B

6.An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack.

What is the reason for this discrepancy?

A. The computer has a HIPS installed on it.

B. The computer has a NIPS installed on it.

C. The computer has a HIDS installed on it.

D. The computer has a NIDS installed on it.

Answer: C

7.A user received a targeted spear-phishing email and identified it as suspicious before opening the content.

To which category of the Cyber Kill Chain model does to this type of event belong?

A. weaponization

B. delivery

C. exploitation

D. reconnaissance

Answer: B

8.What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.

B. Untampered images are deliberately altered to preserve as evidence.

C. Tampered images are used as evidence.

D. Untampered images are used for forensic investigations.

Answer: D

Explanation:

The disk image must be intact for forensics analysis. As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process. Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

9.What is the difference between an attack vector and attack surface?

A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.

B. An attack vector identifies components that can be exploited, and an attack surface identifies the potential path an attack can take to penetrate the network.

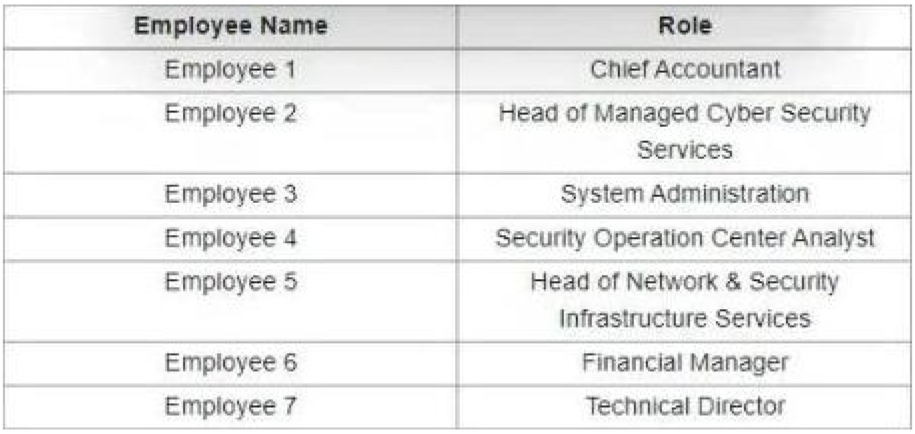
C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.

D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

Answer: C

10.Which process is used when IPS events are removed to improve data integrity?
A. data availability
B. data normalization
C. data signature
D. data protection
Answer: B

11.Refer to the exhibit.



Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

Which stakeholders must be involved when a company workstation is compromised?
A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
B. Employee 1, Employee 2, Employee 4, Employee 5
C. Employee 4, Employee 6, Employee 7
D. Employee 2, Employee 3, Employee 4, Employee 5
Answer: D

12.What is the function of a command and control server?
A. It enumerates open ports on a network device
B. It drops secondary payload into malware
C. It is used to regain control of the network after a compromise
D. It sends instruction to a compromised system
Answer: D

13.At which layer is deep packet inspection investigated on a firewall?
A. internet
B. transport
C. application
D. data link
Answer: C